medcrypt

MARCH 2022 UPDATE

WHAT THE MEDICAL DEVICE INDUSTRY CAN LEARN FROM PAST CYBERSECURITY VULNERABILITY DISCLOSURES

Since the FDA released their Postmarket Cybersecurity Guidance in 2016, the monthly rate of ICS-CERT medical device advisories has increased by 490%, but appears to have plateaued.

**This is an updated version (2022) of our original 2018 whitepaper analyzing trends in cybersecurity vulnerability disclosures.*

EXECUTIVE SUMMARY

What we found

From our analysis of ICS-CERT advisories, we found and predict:

User authentication issues were the most common root cause of 2021 vulnerabilities

Although cybersecurity has evolved rapidly over the last decade, since we began looking at vulnerability disclosures for medical devices in ICS-CERT 4 years ago, the most common root cause of these vulnerabilities has been in user-authentication mis-management. This trajectory suggests that we would expect future advisories to focus on deeper "layers" of the technology stack as medical device cybersecurity matures.

Pervasive vulnerabilities, like log4jshell, did not consistently result in advisories. We expected a strong correlation, as with other industrial control systems using ICS-CERT

Advisories reporting low-level/pervasive vulnerabilities are not as common as we anticipated and in comparison to industrial control systems reporting vulnerabilities on ICS-CERT. This could be because medical device vendors don't believe a vulnerability in a supporting software platform or application necessitates a disclosure on their part, as further validated by the single operating system related vulnerabilities disclosed in 2021.

After a sharp rise in vulnerability disclosures caused by FDA's 2016 postmarket cybersecurity guidance publication, the rate of advisories appears to have plateaued[1]

The nature of the vulnerabilities disclosed suggests the industry is early in its cybersecurity disclosure evolution. Some of the more deeply technical kinds of vulnerabilities found in other industries participating in ICS-CERT threat sharing have yet to be seen in the medical device disclosure data. Over time as vulnerability management programs mature, the rate of advisories is expected to increase.

The presence of advisories indicates an operational/mature product security process.

Issuing vulnerability advisories should not be interpreted as a security weakness of the underlying product, but instead reflects active engagement in maintaining the cybersecurity posture of a device in the post-market.

---

1 Note that per National Vulnerability Database (NVD) the number of disclosed software component vulnerabilities showed a significant increase from 2016 to 2017, which could be an additional contributor to the increase of ICS-CERT advisories. (https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time)

Why we wrote this report

Many security vendors use fear, uncertainty, and doubt as part of a sales tactic. That isn't how we operate. In an effort to find data to substantiate our view of the space, we turned to vulnerability disclosures. We think data-driven insights provide actionable learnings for all device manufacturers, regardless of size/clinical focus or otherwise. And by sharing the data openly, we hope to collaborate with others interested in making evidence-based security decisions.

What we recommend

Vulnerability management can be difficult and time-consuming, but there are opportunities for improvement, better business value, and ROI at every stage of maturity. The dozens of low level, pervasive vulnerabilities that have impacted medical devices in recent years (think: Urgent/11) demonstrate that all companies need to be prepared. There are enough incentives (including President Biden's executive order and FDA's increased scrutiny on vulnerability management), that the time to mature your programs is now.

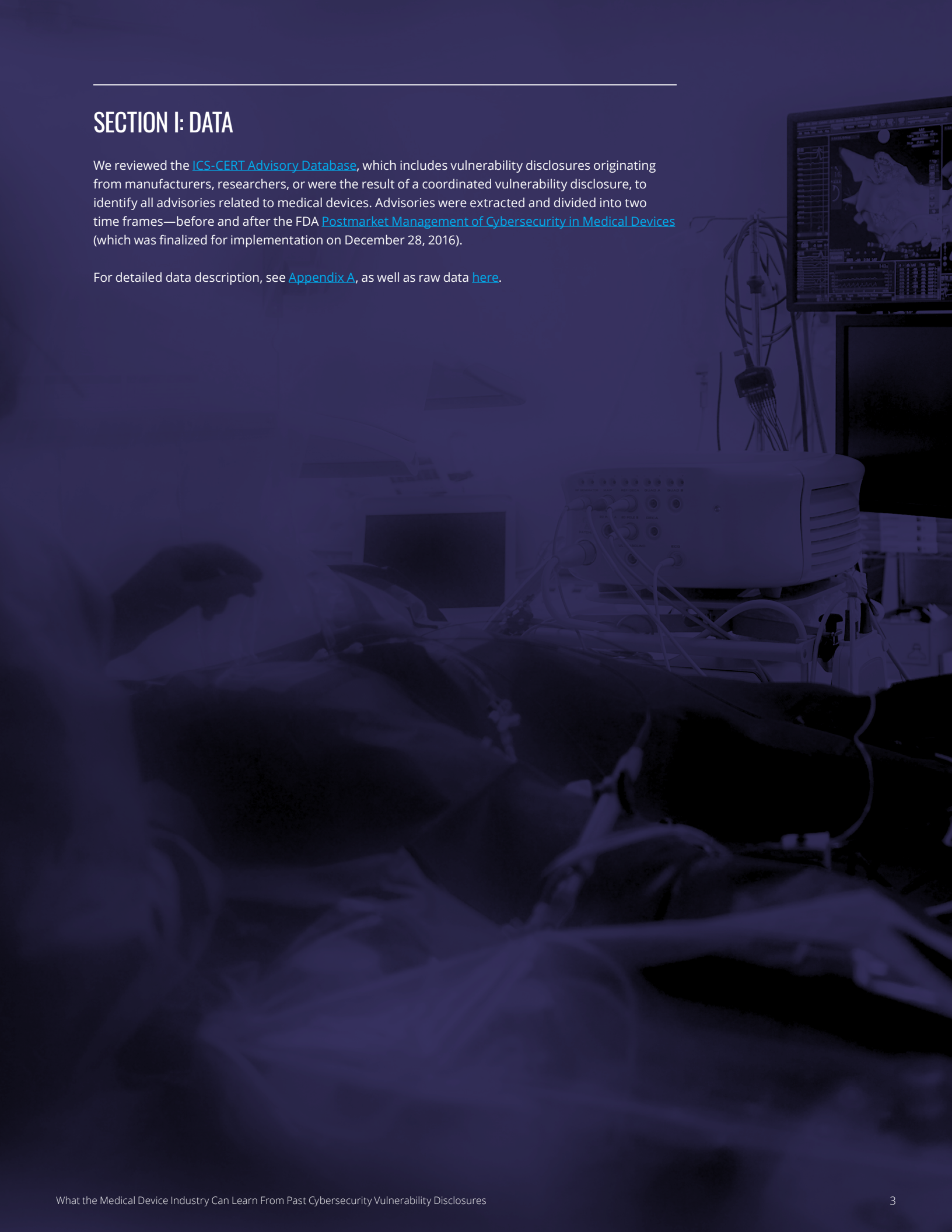
A note on the inclusion of vendor names

We consider the inclusion of a specific medical device manufacturer's (MDM) name in the list of companies below to be a positive indicator of their active management of cybersecurity risk. All technology carries cybersecurity risk, therefore the sharing of medical device cybersecurity advisories is a positive and expected outcome of MDM's postmarket cybersecurity management. Medical device manufacturers who actively disclose and address cybersecurity vulnerabilities should be applauded for embracing and applying resources to the disclosure and sharing process.

SECTION I: DATA

We reviewed the ICS-CERT Advisory Database, which includes vulnerability disclosures originating from manufacturers, researchers, or were the result of a coordinated vulnerability disclosure, to identify all advisories related to medical devices. Advisories were extracted and divided into two time frames—before and after the FDA Postmarket Management of Cybersecurity in Medical Devices (which was finalized for implementation on December 28, 2016).

For detailed data description, see Appendix A, as well as raw data here.



SECTION II: OBSERVATIONS FROM THE DATA

Anatomy of an ICS-CERT Advisory and Recommendations for Extension

The ICS-CERT captures vulnerabilities disclosed since 1999, and supports coordinated sharing of vulnerability disclosures across industrial control systems and medical devices. The ICS-CERT format contains standard fields: vulnerability overview, risk evaluation, affected products, applicable common weakness enumeration (CWE), researcher identification, and finally a mitigations section.

Since MDMs use ICS-CERT as a medium for communicating vulnerability disclosures, we wanted to assess the efficacy of this format. In reviewing the vulnerabilities disclosed, there is a consistent limit of technical and clinical depth, particularly with regards to impact potential.

To make ICS-CERT advisories more beneficial for medical devices/healthcare, additional considerations should be made for understanding how devices are deployed inside healthcare delivery organization (HDO) infrastructure, impact on ability to delivery care as a result of the vulnerability, expectation of mitigation impacting clinical operation, and perhaps messaging for providers/patients to inform while balanced with cybersecurity awareness.

Device Type and Manufacturer

Advisories tend to focus on specific device classes, like pacemakers, insulin and infusion pumps, and imaging systems **(See Exhibit: 1)**. Outside of advisories issued by GE and Philips, certain classes of medical devices are absent in the history of ICS-CERT advisories, in particular surgical robots, radiation oncology, and clinical decision support systems.

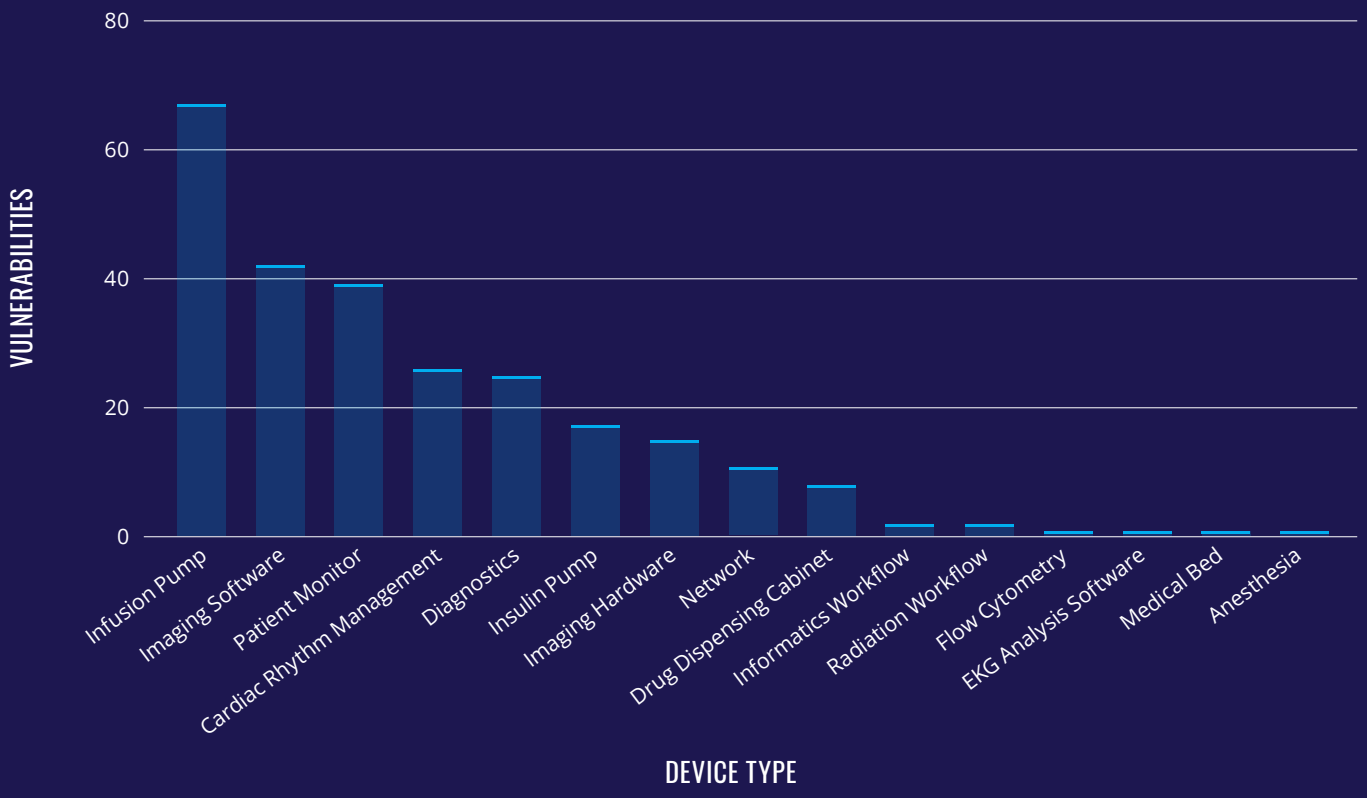


EXHIBIT 1: VULNERABILITIES BY DEVICE TYPE

Relationship Between Device Type and CVSS

We were curious whether the clinical intervention a device supports would be reflected in the related CVSS score associated with a vulnerability. As noted in the graph below, more frequent critical vulnerabilities seem to focus around imaging hardware, imaging software, and patient monitoring devices. The imaging-related vulnerabilities are especially interesting as they're unlikely to be characterized as life-sustaining devices, but their operation would directly impact the delivery of care.

TYPE OF DEVICE	COUNT OF VULNERABILITY DISCLOSURES BY CVSS SEVERITY			
	CRITICAL	HIGH	MEDIUM	LOW
Anesthesia	0	0	1	0
Cardiac Rhythm Management	1	9	14	1
Diagnostics	4	10	11	0
Drug Dispensing Cabinet	0	2	4	1
EKG Analysis Software	0	0	0	1
Flow Cytometry	0	0	1	0
Imaging Hardware	8	1	3	3
Imaging Software	6	11	22	2
Informatics Workflow	0	0	2	0
Infusion Pump	4	36	25	1
Insulin Pump	0	3	14	0
Medical Bed	0	0	1	0
Network	3	7	1	0
Patient Monitor	6	5	25	3
Radiation Workflow	1	1	0	0

EXHIBIT 2: COUNT OF VULNERABILITY DISCLOSURES FOR DEVICE TYPES BY CVSS SEVERITY

* Note: line items within an advisory that did not include a detailed CVSS score, had too many CWEs to assess as a collective or did not reference a related CVSS version in scoring (labeled at TM1 in raw data) have been excluded from this analysis.

Pervasive Vulnerabilities and Vulnerability Disclosures

Vulnerabilities affecting the Windows OS, hardware components like memory controllers and CPUs, Bluetooth interfaces, and various TCP/IP network stacks have been publicly disclosed, all of which are readily used across the healthcare ecosystem. In 2021 alone, we observed several high-impact vulnerabilities like BadAlloc, Nucleus:13, Ripple20, Amnesia:33, and Log4Shell.

We hypothesized that the prevalence of these types of deeply embedded supply chain vulnerabilities would result in a commensurate increase in device or technology-specific disclosures by MDMs. However, we found **no demonstrated impact** of broad impact vulnerabilities on ICS-CERT advisories.

This isn't to say that MDMs did not discuss these pervasive vulnerabilities, just that the ICS-CERT process is not what was used to do so. In fact, 15 of the top 40 MDMs (by revenue) have a specific reference on their website to at least one of the high-impact vulnerabilities that occurred in 2021. With regards to Log4Shell in particular, 5 out of 5 of those impacted devices referenced a mitigation strategy, no small feat given the wide distribution and deeply embedded nature of the affected software tool!

Some Companies Have Yet to Issue an Advisory

Comparing the list of companies who have made disclosures against a list of device vendors ranked by market cap, of the top 40 medical device vendors, 16 have a published vulnerability disclosure process, which includes both a mechanism to intake feedback and communicate findings. Also, 18 of the top medical technology vendors that have connected devices in their portfolio have never made a disclosure through ICS-CERT.[2] We would expect that companies with more mature vulnerability disclosure programs would have a greater number of advisories, as indicated by the fact that more than half (58/110) of disclosures coming from 3 companies alone (BD, Medtronic, Philips).

2 This analysis did not comprehensively look at MDM product security website communications

There are at least three plausible reasons a medical device vendor wouldn't have issued an ICS-CERT disclosure.

1. The device is not connected. Of the top 40 medical device vendors 8 do not offer products that are computerized or connected to a health system network.

2. Communication of the vulnerability and/or fix wasn't made public. There is no law or regulation that states that MDMs must disclose vulnerabilities publicly (unless subject to regulatory recall, corrective action, or removal) therefore it is reasonable to assume that some MDMs simply contact their customers directly rather than putting out full public disclosures.

   Of those 16 manufacturers with disclosure processes, 3 have not made a vulnerability disclosure through the ICS-CERT database. We consider the existence of a disclosure policy to the "crawl" step of a maturing process. This provides a welcome to researchers and processes internally for receiving a vulnerability report from an external source. Having a disclosure policy is positive for healthcare security, if it has not yet been used.

3. They have never been made aware of or discovered a vulnerability.

   Vendors who have yet to issue an advisory due to lack of vulnerabilities should continue to evolve their product development processes including methods for evaluating flaws in architecture and implementation, as well as postmarket monitoring. While internal processes and resources are maturing it may be helpful for MDMs to engage with external resources that specialize in vulnerability discovery and management.

Role of Researchers

Of the 122 advisories assessed, 87 (71%) explicitly referenced a researcher[3] being involved in the identification of the vulnerability. Historically, researchers have been viewed as adversaries, but their attribution in a majority of advisories confirms their persistent presence in the ecosystem **(See Exhibit: 3)**.

RESEARCHER EXPLICITLY REFERENCED	POST - FDA	PRE - FDA	GRAND TOTAL
No	34	1	35
Yes	76	11	87
Grand Total	**110**	**12**	**122**

EXHIBIT 3: COUNT OF RESEARCHER REFERENCES IN ADVISORIES

3 Note - this is not meant to imply that researchers were not involved in other ICS-CERT vulnerability disclosures, only that researchers were explicitly referenced in 28 vulnerabilities prior to FDA guidance and 153 since the guidance was issued.

One of the hypotheses we've put forth in the past was accessibility to devices relating to where researchers are active. Top ranking for researcher referenced vulnerabilities relate to infusion pumps and patient monitors, supporting this idea **(See Exhibit: 4)**.

TYPE OF DEVICE	RESEARCHER EXPLICITLY REFERENCED		GRAND TOTAL
	NO	YES	
Anesthesia	0	1	1
Cardiac Rhythm Management	3	9	12
Diagnostics	3	5	8
Drug Dispensing Cabinet	1	4	5
EKG Analysis Software	1	0	1
Flow Cytometry	1	0	1
Imaging Hardware	4	4	8
Imaging Software	6	7	13
Informatics Workflow	0	1	1
Infusion Pump	6	13	19
Insulin Pump	0	6	6
Medical Bed	0	1	1
Network	0	1	1
Other	9	21	30
Patient Monitor	1	13	14
Radiation Workflow	0	1	1
Grand Total	**35**	**87**	**122**

EXHIBIT 4: COUNT OF RESEARCHER REFERENCES BY DEVICE TYPES

Root Causes Haven't Changed

Vulnerabilities attributed to user authentication and code defects covered 61.4% of the vulnerabilities included in the ICS-CERT advisories after January 1, 2017. This seems indicative of a historical way of working in healthcare assuming trust in the operator of a device or a third party library without ongoing maintenance. It's all been true since we started doing this analysis that year over year, these two are the most frequent drivers for vulnerability disclosures.

Only 22% Percentage of Advisories Did Not Address Patching

Prior to the FDA postmarket guidance, the frequency of patching being referenced in an advisory was 48.6%. Since then, it has almost reached 80%. This indicated not only growing maturity in the vulnerability intake process but also MDMs willingness to address vulnerabilities through patches and updates.

But what happens once a patch is available? If we look at today's approach, there are practical restraints on the healthcare delivery organization (HDO) side that limit the effectiveness of medical device security programs. Although notable efforts exist to gain visibility into patch availability, implementation and risk management in a clinical setting, so far they have been idiosyncratic. HDO's patch management is largely reactive and process driven (e.g., depending on vulnerability disclosure and patch distribution), or limited to addressing the problem "on the outside" through network-based anomaly detection solutions. Certainly, a worthwhile effort but still limited in effectiveness and impact.

Currently, there are significant barriers to implementing patches in the HDO, when they're available from the MDM. Primarily, that the device may be in use for extended periods, or that the device is actually updated physically by the staff of the MDM. Both of which could contribute to significant delays between disclosure, patch issue, and patch implementation. Unfortunately, the timeliness of patching couldn't be evaluated with the ICS-CERT data set. Does this reactive approach provide a sufficiently secure state across the industry? It's reasonable to assume that we won't be able to patch fast enough and complete enough to become secure enough and therefore, as an industry, need to shift to a more proactive security approach.

SECTION III: CONCLUSIONS & PREDICTIONS

Based on the analysis performed as well as our experience in the industry we do want to share a number of hypotheses and predictions that may be of interest for further observation.

HYPOTHESIS	MEDCRYPT VIEW
A wide range of manufacturers have not embraced vulnerability disclosures through ICS-CERT. Vulnerability disclosures have reached a plateau and without additional steps by regulators or device consumers, may never mature beyond the current level.	ICS-CERT disclosures are perceived as an after action communication with limited usability for consumers of medical devices. A meaningful change in device market readiness dynamics will need to occur to prioritize security for all stakeholder acceptance.
At the current pace of cyber risk evolution, today's security processes/approaches/strategies will not lead to sufficient security posture of the industry.	We have not made sufficient progress in the last 5 years to change the balance in favor of defenders. A fundamental approach shift to be more proactive/ earlier in the supply chain must be adopted for widespread impact.
There is a harmful disconnect between device development and postmarket vulnerability management, as noted by the absence of technical/actionable engineering insights in individual vulnerability disclosures.	Vulnerability disclosures with sufficient engineering details would indicate a mature operational security program, but should not be considered reflective of premarket security design considerations. Perhaps with time, and maturity, new measures to help us assess the state of security will evolve.
The increase in the number of vulnerabilities per advisory in recent years, reflects greater depth in analysis of impact on a device.	As vulnerability disclosure matures, an assessment of impact of vulnerabilities on each other, and thus collectively on a device, would better indicate actual risk.
Manufacturers are not incentivized to use the ICS-CERT as part of the disclosure process, with pervasive vulnerabilities serving as an example of not having done so. We believe that unless an ICS-CERT is somehow supportive/additive to a resolution, it is unlikely to be published.	As cybersecurity matures and manufacturers are able to patch more efficiently and effectively, there will be less of a need for vulnerabilities to be disclosed via the ICS-CERT process.

DISCLOSURES

The authors of this paper are employed by MedCrypt Inc, a medical device cybersecurity solutions.

APPENDIX A - DETAILED DATA DESCRIPTION

Vulnerability Disclosure Frequency

	OCTOBER 2013 TO DECEMBER 2016	JANUARY 2017 TO DECEMBER 2021
Number of Advisories	12	110
Total Vulnerabilities Disclosed in Advisories	37	314
Average Advisories per month	0.31	1.83
Average Vulnerabilities per month	0.95	5.23
Companies (advisories issued)	Animas, Baxter, Carefusion (2), Hospira (5), Philips (2), Smiths Medical	Abbott Laboratories (2), B. Braun (4), Baxter (4), BeaconMedaes, Becton, Dickinson and Company (12), Biosense Webster Inc. / Johnson & Johnson, BIOTRONIK, BMC, Boston Scientific (2), Carestream, Change Healthcare (2), Dräger, ENEA/Green Hills Software/ITRON/IP Infusion/ Wind River, Ethicon Endo-Surgery/ Johnson & Johnson, Fresenius, Fujifilm, GE (5), Hamilton Medical AG, Hillrom (2), i-SENS, Innokas Yhtymä Oy, Insulet, Medtronic (11), Natus Medical, Inc., OpenClinic GA, Philips (35), Qualcomm Life, Roche, Siemens (2), Silex Technology/GE Healthcare, Smiths Medical, SOOIL Developments Co., Spacelabs, St. Jude, Stryker, Swisslog Healthcare, Vyaire, Ypsomed, Zoll
Mean Vulnerabilities' CVSS Score	7.30	6.81[4]

EXHIBIT: 5

4 For the period after the FDA guidance was issued it is noted that the version of CVSS methodology used was consistently version 3.

Advisory Frequency vs. ICS-CERT ID Year

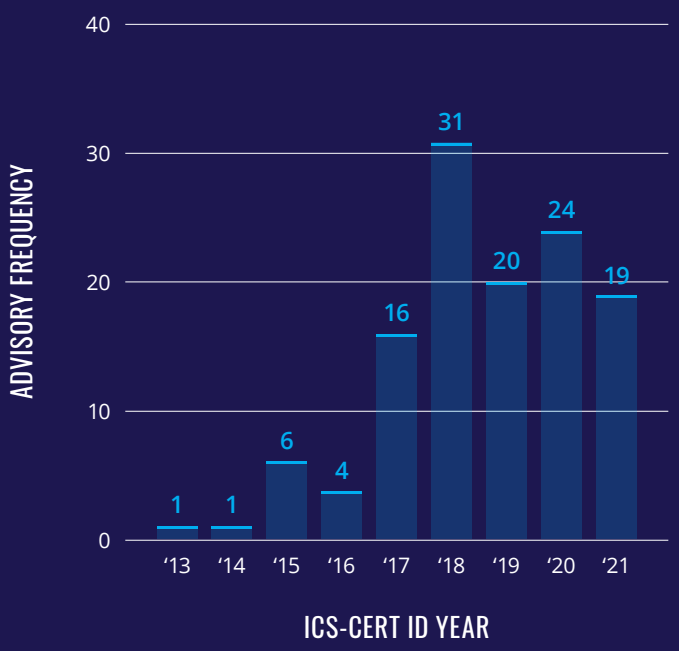


EXHIBIT: 6

Vulnerability Frequency vs. ICS-CERT ID Year

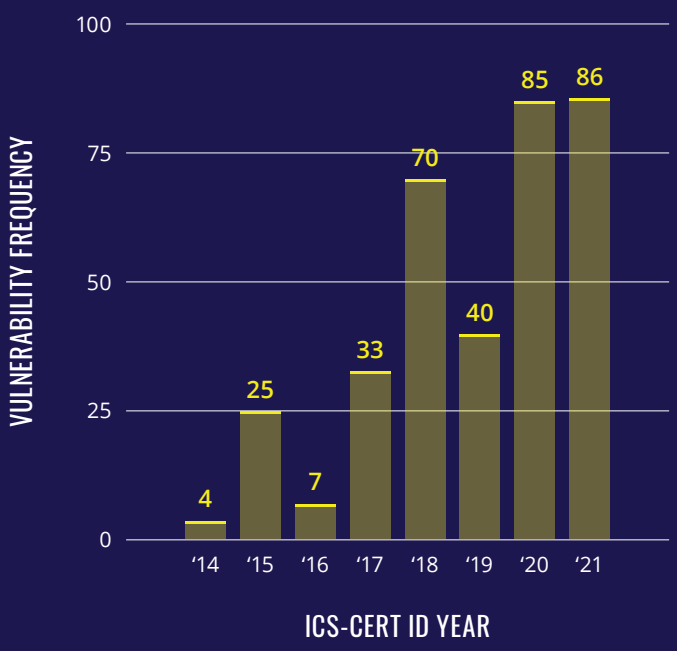


EXHIBIT: 7

Despite not mandated by law, the number of published vulnerabilities has increased since the release of the FDA Postmarket Guidance, with an average of 5.23 vulnerabilities being released per month, compared to 0.95 per month prior to December 2016. Specifically, applying the National Vulnerability Database (NVD) criteria, details of which are included in Appendix B, the severity of vulnerabilities were expressed as a percentage of the total vulnerabilities disclosed for a time period, as noted in the graphic below **(See Exhibit: 9)**.

The timing of FDA guidance demonstrates a pivot point after which there was a large increase in critical and medium risk disclosures, along with a decrease in high-risk vulnerabilities disclosed. This is particularly impressive since there is no specific disclosure law for MDMs, which means that medical device manufacturers (MDMs) view guidance and other factors as market incentives.

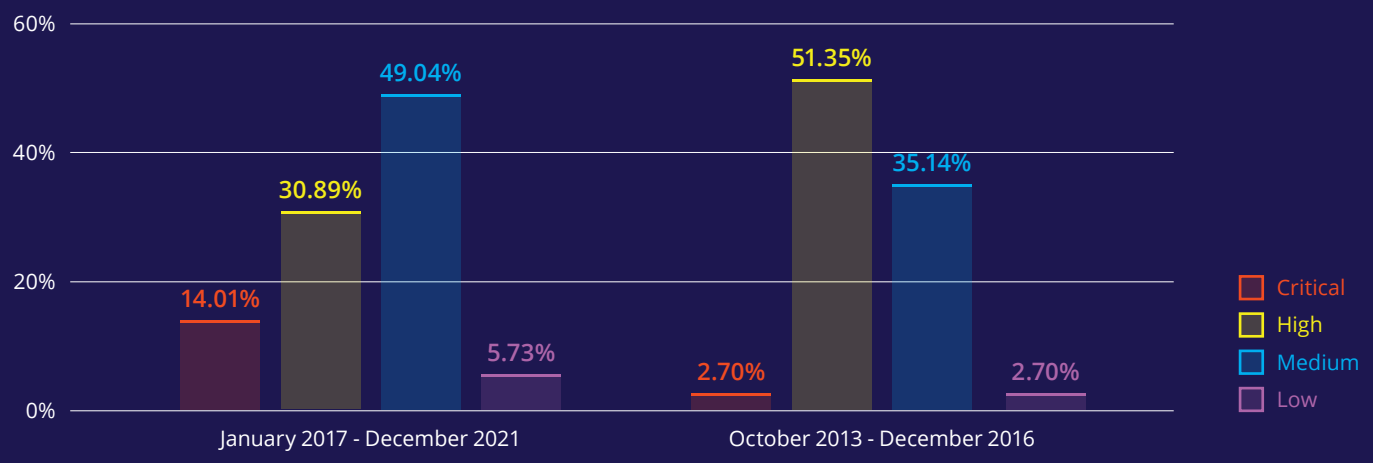


EXHIBIT: 8 | Note: Those advisories which did not include a detailed CVSS score breakdown or did not reference a related CVSS version in scoring were excluded from analysis.

Vulnerability Causes

We attempted to sort the disclosures into eight categories of technological root causes **(See Exhibit: 9)**. While many of the vulnerabilities have aspects of multiple categories, we've matched each common weakness enumeration (CWE) (or common vulnerability exposure (CVE) if a CWE was not referenced in the advisory) with one category. (Please see Appendix C for an explanation of each category.)

ATTRIBUTED ROOT CAUSE	OCTOBER 2013-DECEMBER 2016 TOTALS	JANUARY 2017-DECEMBER 2021 TOTALS
Code Defect	5	63
Encryption	8	42
Operating System Vulnerability	1	24
System Configuration	4	36
Third Party Library	3	10
Third Party Encryption		2
User Authentication	16	130
Misc		7
Grand Total	**37**	**314**

EXHIBIT: 9

Role of Security Researchers

Since the first medical device security researcher shared their findings, the role of security researchers in healthcare cybersecurity has continued to evolve. While there are stories of researcher's work that have splashed across mainstream media headlines, the medical device community at large, including regulators, has gone through great efforts to build a trusted and collaborative relationship between researchers and device manufacturers **(See Exhibit: 10).**

RESEARCHER EXPLICITLY REFERENCED	POST - FDA	PRE - FDA	GRAND TOTAL
No	34	1	35
Yes	76	11	87
Grand Total	**110**	**12**	**122**

EXHIBIT: 10

Correlation of CVSS to Root Cause

CVSS scores can draw a visceral response from the healthcare industry because CVSS scores are an approximation of risk, but in practice they often don't correlate well with realized risk, exploitability etc. Conceptually, CVSS can help prioritize mitigations by incorporating exploitability risk factors into overall decision making, and FDA recommends the use of CVSS in their postmarket guidance **(See Exhibit: 11)**.

Patching as a Mitigation

Currently, disclosure is a complex mechanism for information sharing to enable risk reduction. Even without a patch or fix, disclosure by technology builders is seen as helping consumers defend against attackers. While there are complications in the healthcare space with respect to patching, patching is seen as a robust risk-reducing method. Since 2016, when the FDA postmarket guidance emphasized the importance of patching, the number of disclosed advisories that received a patch increased by 1.5x - with 77.3% of advisories being patched in 2020 **(See Exhibit: 12)**.

Prevalence of broad impact vulnerabilities

Please note that there was one vulnerability in 2019 that stood out as resulting in a unique advisory, ICSMA 19-274 (describing CVE-2019-12256 through -12265, collectively known as Urgent/11), as it described a set of vulnerabilities of a third party software product rather than an actual finished medical device. We did not change our methodology because of this single occurrence, but wanted to clarify this to the readers' benefit.

Median CVSS[5] Value

ROOT CAUSE	TIMELINE RELATIVE TO FDA GUIDANCE	
	POST - FDA	**PRE - FDA**
Code Defect	6.8	7.6
Encryption	6.4	6.4
Misc	4.9	0
Operating System Vulnerability	7.3	7.0
System Configuration	6.3	7.5
Third Party (Encryption)	5.9	0
Third Party Library	7.9	8.4
User Authentication	7.1	8.1

EXHIBIT: 11

Advisories that list patching as a mitigation

	NOT LISTED	LISTED
No	60	254
Yes	18	19
Grand Total	**78**	**273**

EXHIBIT: 12

5 When looking at trending CVSS scores or comparison of CVSS scores across categories we can choose statistical methods that describe a central or representative value of a group of numbers. The Median has been assessed as it is the preferred measure when describing data sets that are skewed or contain significant outliers.

APPENDIX B

Assessment on CVSS Versions

CVSS transitioned from version 2.0 to version 3.0 during the period from October 2013 to December 28, 2016, the details of which are outlined below **(See Exhibit: 13)**.

CVSS V3 RATINGS

1. Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
2. Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
3. Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-8.9.
4. Vulnerabilities will be labeled "Critical" severity if they have a CVSS base score of 9.0-10.0.

CVSS V2 RATINGS

1. Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
2. Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
3. Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

EXHIBIT: 13

The advisories under review were bucketed into qualitative ranges based on the NVD criteria outlined below **(See Exhibit: 14)**. Where a version of CVSS was not referenced or hundreds of vulnerabilities were included in a single advisory (see TM1 in raw data), these were excluded from the assessment.

TIMELINE RELATIVE TO FDA GUIDANCE	CRITICAL	HIGH	MEDIUM	LOW	TM1	GRAND TOTAL
Post - FDA	44	97	154	18	1	314
Pre - FDA	1	19	13	1	3	37
Grand Total	**45**	**116**	**167**	**19**	**4**	**351**

EXHIBIT: 14

The assessment of the new version by Omar Santos, Cisco, predicted in 'The Evolution of Scoring Security Vulnerabilities', an increase in high and critical findings under version 3. The medical device advisories demonstrated a shift in more medium categorizations between version 2 and 3 **(See Exhibit: 15)**. This may be an indicator that even with an increase in vulnerabilities reported, the reported vulnerabilities were lower risk, perhaps further corroborating alignment with fewer technical findings.

	VERSION 3 COUNT	VERSION 3 PERCENTAGE	VERSION 2 COUNT	VERSION 2 PERCENTAGE
Critical	23	16%	0	0
High	47	32%	17	61%
Medium	72	49%	10	36%
Low	5	3%	1	4%

EXHIBIT: 15

Specifically as outlined in Appendix B, the common vulnerabilities (CWE IDs) anticipated to cause increases are buffering and user authentications, which are notably attributed as the root cause for many of the medical device advisories.

APPENDIX C

Description of Vulnerability Cause Categories

Code Defect	Can be described as imperfect implementations of otherwise secure software designs. An example of a code defect would be a Buffer Overflow. Many of these defects can be identified in the verification and validation process using tools like Static Code Analysis and Fuzz Testing.
Encryption	The lack of encryption of sensitive data, or vulnerabilities in the way this encryption is implemented, can leave devices and data vulnerable to attack. Common examples are storing user credentials in plain text, storing encryption keys in an insecure fashion, or vulnerabilities discovered in the underlying encryption software and algorithms.
Operating System Vulnerability	Many medical devices include computers running retail operating systems, like Microsoft Windows. These operating systems are regularly found to have vulnerabilities unrelated to the medical device itself, but that can affect the function of the device if left unpatched. One example would be the March 2017 "EternalBlue" vulnerability in Microsoft Windows handling of SMB transactions.
User Authentication	Failure to require user authentication for critical functions, or vulnerabilities in the way users are authenticated, can leave devices susceptible to attack. One common example is the use of "hard-coded" user credentials used across a fleet of devices.
System Configuration	Connected medical devices and their underlying software systems can be designed "securely", but configured in a way that leaves a device susceptible to attack. A common example is failing to disable unnecessary OS services and block all unused ports.
Third Party Library	Medical devices frequently rely on third party software for critical functions, which can be found to have vulnerabilities. One example would be a medical device including a version of a database server application found to have a publicly disclosed vulnerability.
Third Party Encryption	Use of a third party hard- or software component that demonstrated a weakness related to its encryption algorithm. (e.g. OpenSSL)
Miscellaneous	Disclosures that did not fit into one of the above categories were labeled "Miscellaneous."

EXHIBIT: 16

medcrypt

MedCrypt provides proactive security for healthcare technology. MedCrypt's platform brings core cybersecurity features to medical devices with just a few lines of code, ensuring devices are secure by design. MedCrypt announced a $5.3 million Series A funding round in May of 2019, bringing the total funds raised to $9.4 million with participation from Eniac Ventures, Section 32, Y Combinator, and more. The company is based in San Diego, California.

For further details, please visit and contact:

Website: www.medcrypt.com
Email: info@medcrypt.com
Twitter: @MedCrypt